CLAIMS

What is claimed is:

1. A method of creating a fault-inducing transaction representation in a network, the method comprising:

interjecting a pattern with fault-inducing sub-fields, where the pattern is an expression including a literal string and a wildcard character class; and

using the expression to form a subsequent expression that can be used by a target system to detect and trigger on the network at least one transaction that matches the expression.

2. An article of manufacture, comprising:

a machine-readable medium having stored thereon instructions to:

interject a pattern with fault-inducing sub-fields, where the pattern is an expression including a literal string and a wildcard character class; and

use the expression to form a subsequent expression that can be used by a target system to detect and trigger on the network at least one transaction that matches the expression.

3. An apparatus for creating a fault-inducing transaction representation in a network, the apparatus comprising:

means for interjecting a pattern with fault-inducing sub-fields, where the pattern is an expression including a literal string and a wildcard character class; and

coupled to the interjecting means, means for using the expression to form a subsequent expression that can be used by a target system to detect and trigger on the network at least one transaction that matches the expression.

4. A method of testing a target in a network by fault injection, the method comprising:

defining a transaction baseline;

modifying at least one of an order and a structure of the transaction baseline to obtain a modified transaction with malformed grammar; and

transmitting the modified transaction to a target.

5. The method of claim 4, further comprising:

after transmitting the modified transaction, receiving a feedback from the target to determine fault occurrence.

6. The method of claim 4 wherein the modifying step comprises:

providing alternative character encoding for a character in the transaction baseline.

7. The method of claim 4 wherein the modifying step comprises:

removing a field from the transaction.

8. The method of claim 4 wherein the modifying step comprises:

duplicating a field in the transaction.

9. The method of claim 4 wherein the modifying step comprises:

creating a double delimiter in the transaction.

10. The method of claim 4 wherein the modifying step comprises:

sending all delimiters in the transaction.

11. The method of claim 4 wherein the modifying step comprises:

sending a blank transaction with no values in the transaction.

12. The method of claim 4 wherein the modifying step comprises:

sending a single character and delimiter-value pair at a repeated large buffer in the transaction.

13. The method of claim 4 wherein the modifying step comprises:

sending an unbalanced pair in the transaction.

14. The method of claim 4 wherein the modifying step comprises:

replacing a delimiter with random ranges that cover the value of the delimiter.

15. The method of claim 4 wherein the modifying step comprises:

using an alternative encoding to encode a transaction field with a character that is equal in nature and different in representation.

16. The method of claim 4 wherein the modifying step comprises:

using prefixed escapes in the transaction.

17. The method of claim 4 wherein the modifying step comprises:

using value injection to alter an input field in the transaction.

18. The method of claim 4 wherein the modifying step comprises:

using ghost character encoding in the transaction.

19. The method of claim 4 wherein the modifying step comprises:

determining a value injection based on numerical ranges of the input field content.

20. The method of claim 4 wherein the modifying step comprises:

controlling the user identity which is a field indicating resource name or user identity.

21. The method of claim 4 wherein the modifying step comprises:

injecting unfiltered metacharacters to a secondary process.

22. The method of claim 4 wherein the modifying step comprises:

using extraneous meta-characters for causing misclassification.

23. The method of claim 4 wherein the modifying step comprises:

parsing out a delimiter to obtain an intermediate representation of the transaction, where a value in the transaction is replaced by a buffer function.

24. A method of testing a target on a network by fault injection, the method comprising:

defining a transaction baseline;

modifying an input field in the transaction baseline to obtain a modified transaction with malformed value; and

transmitting the modified transaction to a target.

25. The method of claim 24, further comprising:

after transmitting the modified transaction, receiving a feedback from the target to determine fault occurrence.

26. The method of claim 24 wherein the modifying the input field in the transaction baseline comprises:

providing a ghost character in the transaction baseline, where the ghost character does not effect the validity of the transaction.

27. A method of testing a target in a network by fault injection, the method comprising:

defining a transaction baseline;

modifying the transaction baseline to obtain a modified transaction with an extraneous metacharacter; and

transmitting the modified transaction to a target.

28. An apparatus for testing a target in a network by fault injection, the apparatus comprising:

a driver configured to generate patterns, where a pattern can generate a plurality of packets for transmission to the target, the pattern being represented by an expression with a literal string and a wild character class; and

a network interface coupled to the driver and configured to transmit and receive network traffic.